Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of claims:

Claims 1-9 (cancelled).

Claim 10 (previously presented). A processor for performing a cryptographic algorithm, the cryptographic algorithm including a modular multiplication of a multiplicand by a multiplier, in which a modulus is employed, wherein the multiplicand, the multiplier, and the modulus are parameters in the cryptographic algorithm, using a multiplication look-ahead process and a reduction look-ahead process, comprising:

a means for transforming the modulus into a transformed modulus being greater than the modulus by multiplying the modulus by a transforming number, the transforming number being calculated using the modulus such that a predetermined fraction of the transformed modulus has a higher-order digit with a first predetermined value followed by at least one lower-order digit having a second predetermined value;

a means for iteratively working off the modular multiplication using the multiplication look-ahead process and the reduction

look-ahead process and utilizing the transformed modulus so as to obtain at the end of the iteration a transformed result for the modular multiplication, the predetermined fraction of the transformed modulus being used in the reduction look-ahead process; and

a means for re-transforming the transformed result by modular reduction of the transformed result utilizing the modulus.

Claim 11 (previously presented). The processor according to claim 10, comprising a host CPU and a coprocessor, said means for transforming the modulus being arranged in the host CPU and said means for iteratively working off the modular multiplication being arranged in the coprocessor.

Claim 12 (previously presented). The processor according to claim 11, wherein the host CPU is a short-number arithmetic-logic unit having a number of digits smaller than or equal to 64, and the coprocessor is a long-number arithmetic-logic unit having a number of digits greater than or equal to 512.

Claim 13 (previously presented). The processor according to claim 10, wherein the means for iteratively working off the modular multiplication includes a register for the transformed

modulus and a register for an intermediate result of the modular multiplication.